GEOMETRIE PROIETTIVE DI CONGRUENZA E GEOMETRIE PROIETTIVE FINITE*

DI

BEPPO LEVI

In una nota † presentata a questa Società il 22 Aprile 1905 e pubblicata nelle Transactions nell'Aprile 1906 i sigg. VEBLEN e BUSSEY hanno portata la loro attenzione sopra la possibilità di costruire uno spazio contenente un numero finito di punti ed in cui valga una geometria proiettiva per la quale siano conservate le principali proprietà dell'ordinaria geometria proiettiva lineare. ‡ Essi hanno pure analizzato qualcuno dei caratteri speciali a tali spazi e ne han data una rappresentazione analitica generale, raccogliendo infine, in un ultimo paragrafo, una bibliografia abbastanza vasta di lavori che più o meno hanno attinenza all'argomento trattato.

Pare di qui che agli autori sia sfuggito un cenno assai rapido, ma sufficientemente esplicito, che sopra queste geometrie e sopra altre assai più generali io diedi fin dal 1904 in una Memoria sopra i "*Fondamenti della metrica proiettiva*" §; ond'io chiedo alla Società il permesso di ricordare qui brevemente i punti della mia memoria che si riferiscono alla questione, aggiungendo ancora alcuni sviluppi che non mi paiono privi d'interesse.

La definizione analitica delle geometrie trattate giustificherà pienamente il nome generico che io ho qui attribuito loro di *geometrie proiettive di congruenza*.

---

* Presented to the Society October 27, 1906. Received for publication October 21, 1906.

† *Finite projective geometries.*

‡ Cfr. particolarmente, loc. cit., § 4, pp. 245–247.

§ Memorie della R. Accademia delle Scienze di Torino, ser. 2, vol. 54 (1904); v. il no. 21, *La geometria proiettiva*, pp. 42–44.

Solo dopo che anche il presente articolo era già stato scritto ebbi esatta conoscenza della Nota dello HESSENBERG: "*Ueber die projektive Geometrie*," Sitzungberichte der Berliner mathematischen Gesellschaft (28 Gennaio 1903), la quale è pur ricordata dai sigg. VEBLEN e BUSSEY (loc. cit., § 9, p. 258). Mi è debito perciò di riconoscere allo HESSENBERG larga parte della priorità qui reclamata, poichè in quella Nota egli afferma con precisione l'independenza della geometria projettiva lineare dalla nozione di ordine, e la dimostra per l'appunto colla costruzione di geometrie projettive finite dei tipi che—seguendo i sigg. VEBLEN e BUSSEY—si chiamerebbero (come sarà tosto ricordato) $PG(2, p)$ e $PG(2, p^2)$. Egli rileva pure (come, independentemente, è avvenuto a me) che in geometrie projettive in cui manchi la nozione d'ordine, divengono possibili configurazioni che sono impossibili nell'ordinario spazio projettivo: —così la configurazione d'un quadrangolo completo coi tre punti diagonali allineati, nella $G(2, 2)$ ed anche in piani contenenti infiniti punti (Cfr. il testo, n. II).

Le osservazioni dello HESSENBERG non invadono però per nulla il campo delle ulteriori considerazioni che sono oggetto del presente scritto.

I. Nella citata Memoria, dopo aver stabiliti, in base ai postulati ammessi, i teoremi di Desargues e di Pascal, onde risultò possibile, seguendo il sig. Hilbert, di riferire lo spazio geometrico ad un sistema di coordinate proiettive, io osservava: *

"Mi piace di rilevare come il concetto di ordine degli elementi di una forma di prima specie non abbia avuto fin qui alcuna parte nella istituzione della nostra geometria e non abbia più alcuna ragione di averne in seguito, in tutto lo sviluppo della geometria proiettiva. . . . È essenziale notare che, per questa costruzione della geometria proiettiva, non è necessario che," nella corrispondenza che la rappresentazione per coordinate stabilisce fra i punti degli assi coordinati dello spazio geometrico ed i numeri del campo numerico, "a espressioni aritmeticamente irreduttibili fra loro di questo campo numerico corrispondano punti † diversi dagli assi . . .; bensì è necessario soltanto che a punti diversi corrispondano numeri o espressioni fra loro aritmeticamente irreduttibili. . . ."

Mediante note operazioni geometriche le quali, sugli assi di uno spazio proiettivo, permettono di costruire il punto la cui coordinata relativa all'asse considerato è la somma, la differenza, il prodotto od il quoto delle coordinate relative a due altri punti assegnati ‡ si possono cioè "costruire tutti i punti degli assi corrispondenti agli elementi del campo di razionalità che ha per base un sistema di segni aritmetici (numeri) § corrispondenti a quanti si vogliano punti fissati arbitrariamente sugli assi. Ora si può supporre che due elementi di questo campo, fra loro aritmeticamente irreduttibili, rappresentino tali successioni di operazioni geometriche che conducano allo stesso punto finale. La differenza di questi due elementi aritmetici rappresenterà allora il punto 0" (origine delle coordinate). "L'insieme di tutti gli elementi rappresentanti questo punto 0 costituisce evidentemente un modulo con coefficienti appartenenti al campo di razionalità sopra nominato; e rappresentano uno stesso punto tutte e sole le espressioni di questo campo di razionalità congrue fra loro rispetto a tal modulo. Il prodotto di due punti p, q non sarà mai lo 0 se non è 0 almeno uno di essi." Il modulo nominato sarà cioè primo.

In tutto quanto segue chiamerò questo modulo *il modulo fondamentale della geometria.*

II. I sigg. VEBLEN e BUSSEY si occupano precisamente di questi spazi in cui le coordinate omogenee dei punti sono gli elementi di un campo di Galois $G(p^n)$; sono cioè i sistemi di polinomi in una variabile x a coefficienti appar-

---

* L. c., p. 42–43.

† Nel testo citato in luogo di punti e assi si parla di raggi e piani coordinati; ciò perchè quelle frasi si riferiscono ad una geometria nella stella.

‡ Cf. HILBERT, *Grundlagen der Geometrie*, § 24–26, ovvero la mia Memoria, no. 17.

§ Forse l'uso che io ho fatto di questa parola "numeri" può aver diminuito la veduta della generalità del concetto nella mente del lettore.

tenenti al campo di integrità naturale,* congruenti rispetto al modulo che ha per elementi fondamentali un numero primo p e un polinomio dato in x di grado n, a coefficienti interi (che si possono sempre supporre $< p$) irreduttibile rispetto al modulo p. Anche per essi i polinomi che costituiscono il modulo rappresentano il punto 0. La geometria di un tale spazio di k dimensioni chiamano una $PG(k, p^n)$.

Si vede come il mio punto di vista comprenda quello dei sigg. VEBLEN e BUSSEY come caso particolare, ma sia assai più generale del loro. E scegliendo convenientemente il modulo fondamentale si può costruire uno spazio proiettivo che, conservando tutte le proprietà lineari che provengono dai soli postulati di appartenenza (*Verknüpfung*), goda ancora di proprietà ben differenti dallo spazio ordinario (in particolare vi manchi la nozione di ordine) *pur possedendo infiniti punti*. Però nemmeno è sfuggito a me il caso particolare notevole presentato dallo spazio con un numero finito di punti:†

"In particolare, se il campo di razionalità considerato è il campo naturale generato dal solo elemento 1, mediante le operazioni di addizione, sottrazione, moltiplicazione e divisione, gli elementi rappresentanti lo 0 saranno tutti quelli della forma $(h/k)n$, dove n è un numero primo e k non è divisibile per n." ‡ Sopra ciascun asse, ciascun punto sarà rappresentato dall'insieme dei numeri razionali che differiscono fra loro per numeri della forma $(h/k)n$, ovvero — e ciò avverrà per un solo punto (il punto all' ∞) su ciascun asse — dall'insieme di tutte le frazioni irreduttibili il cui denominatore è multiplo di n.

Data una frazione irreduttibile p/q il cui denominatore non sia multiplo di n, si possono sempre trovare due numeri interi positivi h, l, tali che $ql - nh = p$ e quindi, $p/q = l - (h/q)n$. Secondo la definizione sopra esposta, l'intero l rappresenterà lo stesso punto che la frazione p/q. Fra i simboli numerici rappresentanti un punto determinato, diverso dal punto all' ∞, di un asse coordinato, esistono dunque sempre dei numeri interi; e poichè rappresenteranno ancora lo stesso punto i numeri l e $l + \lambda n$, ove λ è un numero intero qualunque, positivo o negativo, potranno sempre questi numeri supporsi $\geqq 0$ e $< n$. Ne risulta che la retta possiedè nella nostra geometria un numero finito $(n + 1)$ di punti. È il caso che i sigg. VEBLEN e BUSSEY rappresentano con $PG(k, n)$. "Se in particolare si fa $n = 2$, si otterrà uno spazio proiettivo . . ." in cui "il quarto armonico dopo tre elementi dati coincide con uno di questi tre.§

*Il fatto che, alla mia considerazione di un campo di razionalità, si sostituisce qui quella di un campo d'integrità dipende da ciò che i sigg. VEBLEN e BUSSEY si riferiscono ad una rappresentazione per coordinate omogenee, oppostamente a quanto avviene nella mia Memoria.

†Spetta però ai sigg. VEBLEN e BUSSEY il merito di essersi posto il problema di definire *tutti* gli spazi proiettivi finiti e di averlo risolto caratterizandoli nei $PG(k, p^n)$ sopra ricordati.

‡V. la mia *Memoria* citata, p. 43. Nelle linee seguenti della stessa p. 43 si ritrovano le stesse considerazioni che qui seguono, in una esposizione che qui parrebbe meno opportuna al l'intelligenza.

§Cfr. la Nota dei sigg. VEBLEN e BUSSEY, § 3.

L'esempio offerto dal sig. FANO per dimostrare l'indipendenza della proposizione: *il quarto armonico dopo tre elementi dati è distinto da ciascuno di essi*, dai postulati di appartenenza è una realizzazione geometrica di questa costruzione analitica"; onde questo mostra che, in mancanza di quel postulato "molte proposizioni non diverrebbero erronee, ma illusorie." * E la costruzione analitica esposta mostra che tal singolarità non è per nulla legata al *numero* dei punti ammessi alla retta; essa può presentarsi anche in uno spazio d'infiniti punti.†

III. Le geometrie proiettive di congruenza, mentre permettono di scoprire fatti nuovi, conciliabili colle ipotesi fondamentali della geometria proiettiva, danno pur modo di interpretare in un campo reale, anche costituito d'un numero finito di punti, fatti che negli spazi proiettivi ordinarii possono verificarsi solo nel campo complesso.

Come le considerazioni che seguono mostreranno con maggior precisione, questo è, in larga misura, un riflesso naturale della teoria dei numeri algebrici del KRONECKER, per la quale ogni numero algebrico (reale o complesso) viene ad identificarsi con una congruenza fra elementi razionali.

Un notevole esempio si è presentato nella mia *Memoria* nella considerazione di una geometria piana del tipo ultimamente descritto con $n = 3$: ‡ il piano proiettivo è allora costituito di 13 punti e si compone di 13 configurazioni di 9 punti identiche alla configurazione dei flessi di una cubica, la qual configurazione, come si sa, è impossibile in un ordinario piano reale.

Sopra un fatto dello stesso ordine hanno portato la loro attenzione i sigg. VEBLEN e BUSSEY: si sa che, sulla retta complessa, cade in difetto la proposizione fondamentale di v. STAUDT che una corrispondenza armonica in cui tre punti coincidano coi loro omologhi è necessariamente l'identità; fu questo il punto di partenza per interessanti ricerche del Prof. SEGRE sopra quelle corrispondenze armoniche che egli chiamò *antiproiettività* e che risultan dal prodotto di trasformazioni proiettive e di una trasformazione per coniugio.§ Ora un fatto analogo si riproduce nelle geometrie finite dei sigg. VEBLEN e BUSSEY. Essi osservano infatti || che i punti d'una retta di una loro geometria si riuniscono in *catene* (analoghe alle catene di v. STAUDT), i punti di ciascuna delle quali si deducono razionalmente da tre punti assegnati qualsiansi della catena medesima: seguendo i nominati autori, se più catene esistono su una stessa

* Cfr. la mia *Memoria* pag. 43–44.

† Cfr. la nota (3) a piè della pag. 43 nella *Memoria* citata.

‡ L. c. no. 31 — *Un piano metrico di* 9 *punti e un piano proiettivo di* 13 — pp. 53–56: questo esempio presenta una particolare importanza nella dimostrazione della compatibilità e delle dipendenze dei postulati della metrica e di quelli della geometria proiettiva.

§ SEGRE, *Un nuovo campo di ricerche geometriche*, Atti della R. Accademia di Torino, 1890.

|| L. c., § 5, pp. 249, 250.

retta, queste si aggruppano in sistemi più vasti (2-*catene*) contenenti ciascuna tutte e sole le catene, combinazioni lineari di due catene del sistema (e queste due catene hanno, in generale, due punti comuni — distinti o coincidenti); se i punti della retta non appartengono tutti alla stessa 2-catena, esistono ancora sulla retta sistemi lineari più vasti di catene (3-*catene*) e così via: tutti i punti di una retta di una $PG(k, p^n)$ costituiscono in tal modo una *n-catena*. Ora i sigg. VEBLEN e BUSSEY mostrano che al teorema di v. STAUDT si può sostituire quest'altro: *Una corrispondenza armonica sopra una retta di una* $PG(k, p^n)$ *non può avere più di* $n+1$ *punti fissi non appartenenti alla stessa* $(n-1)$-*catena senza ridursi all'identità.**

Questa proposizione stabilisce però per il numero dei punti fissi un limite molto superiore al reale. Io mi propongo di dimostrare, nelle pagine seguenti, che essa può esser sostituita con un'altra assai più precisa.

Mi permetterò anzi di svolgere al riguardo alcune considerazioni generali, da cui si vedrà come si apra qui un largo campo di ricerche algebrico-geometriche.

IV. Sia m una retta di un qualsiasi spazio proiettivo: assegnati arbitrariamente sopra la retta tre punti a, b, c, si può sempre — al più mediante una sostituzione lineare i cui coefficienti siano espressioni razionali nelle coordinate dei tre punti a, b, c — assumere la retta m come asse coordinate fare in modo che le ascisse dei tre punti a, b, c, siano rispettivamente $0, 1, \frac{1}{0} (= \infty)$.† Se allora ξ è l'ascissa di un punto mobile della retta, $\phi(\xi)$ l'ascissa del punto corrispondente per una determinata trasformazione armonica ‡ che tenga fissi i punti a, b, c, è noto § che la $\phi(\xi)$ deve essere una funzione di ξ che soddisfi alle equazioni funzionali

$$(1) \qquad \begin{cases} \phi(\xi+\eta) = \phi(\xi) + \phi(\eta), \\ \phi(\xi^2) = [\phi(\xi)]^2. \end{cases}$$

Reciprocamente ogni funzione ϕ soddisfacente alle equazioni (1) definisce una trasformazione armonica della retta che muta in sè i punti a, b, c. Invero dalla 1ª delle (1) segue

$$\phi(\xi) = \phi(\xi + 0) = \phi(\xi) + \phi(0)$$

onde

$$\phi(0) = 0;$$

$$\phi(\tfrac{1}{0}) = \phi(\xi + \tfrac{1}{0}) = \phi(\xi) + \phi(\tfrac{1}{0})$$

* L. c., § 5, p. 250.

† Dò la preferenza al segno $\frac{1}{0}$ sopra al segno ∞ perchè non nasca alcun dubbio sulla validità dei presenti sviluppi per geometrie finite o, in generale, geometrie nei cui punti non abbiano rappresentazione tutti i numeri reali.

‡ Cioè una trasformazione biunivoca della retta in sè, che muti gruppi armonici in gruppi armonici.

§ DARBOUX, *Sur le théorème fondamental de la géométrie projective*, Mathematische Annalen, vol. 17 (1880), p. 55 (Vedi p. 56-58).

e quindi, poichè non è costantemente $\phi(\xi) = 0$,

$$\phi(\tfrac{1}{0}) = \tfrac{1}{0};$$

infine da

$$\phi(1) = \phi(1^2) = [\phi(1)]^2 \qquad \text{segue} \qquad \phi(1) = 1,$$

e da

$$\phi(0) = \phi(1-1) = \phi(1) + \phi(-1) \qquad \text{segue allora} \qquad \phi(-1) = -1.$$

Si ha inoltre

$$\begin{aligned}\phi[(\xi+\eta)^2] &= \phi(\xi^2+\eta^2+2\xi\eta) = [\phi(\xi)]^2 + [\phi(\eta)]^2 + 2\phi(\xi\eta)\\ &= [\phi(\xi)+\phi(\eta)]^2 = [\phi(\xi)]^2 + [\phi(\eta)]^2 + 2\phi(\xi)\phi(\eta)\end{aligned}$$

onde

$$\phi(\xi\eta) = \phi(\xi)\phi(\eta).$$

Dalle due relazioni

$$\phi(\xi+\eta) = \phi(\xi)+\phi(\eta), \qquad \phi(\xi\eta) = \phi(\xi)\phi(\eta)$$

segue che, se $\xi, \eta, \zeta, \cdots$ sono ascisse di punti qualsivogliano della retta, e $f(\xi, \eta, \zeta \cdots)$ una loro funzione razionale a coefficienti razionali,

(2) $$\phi[f(\xi, \eta, \zeta \cdots)] = f[\phi(\xi), \phi(\eta), \phi(\zeta), \cdots].$$

In questa relazione (2) sono comprese le (1) come caso particolare: essa può quindi sostituirsi al loro sistema. Se allora ξ, η, ζ, θ sono tali che

$$(\xi\eta\zeta\theta) = -1,$$

la (2) ci dice che

$$\phi(-1) = \phi[(\xi\eta\zeta\theta)] = [\phi(\xi)\,\phi(\eta)\,\phi(\zeta)\,\phi(\theta)],$$

ossia

$$[\phi(\xi)\,\phi(\eta)\,\phi(\zeta)\,\phi(\theta)] = -1,$$

con che si prova che la trasformazione considerata è armonica.

V. Ciò posto si consideri una geometria proiettiva tale che le ascisse dei punti generici della retta m siano funzioni razionali a coefficienti razionali delle ascisse di un certo sistema di punti. Solo per ragion di semplicità e per le applicazioni successive supporremo che questi punti siano in numero finito.* Indicheremo inoltre, d'ora innanzi, i punti della retta m e le loro ascisse cogli

* L'ipotesi del numero finito di punti razionalmente independenti non è per nulla essenziale; tra l'altro potrebbero i coefficienti, anzichè essere razionali, appartenere ad un determinato campo ortoide (KÖNIG, *Einleitung in die allgemeine Theorie der algebraischen Grössen*, Leipzig, Teubner, 1903, p. 7–8), per esempio, esser semplicemente reali. Però l'ipotesi della razionalità dei coefficienti è necessaria per qualcuna delle considerazioni seguenti; qualche altra chiede poche ovvie modificazioni nell'ipotesi contraria. Inoltre molte delle conseguenze che da quanto segue possono trarsi divengono illusorie se non si ammette almeno che l'aggregato dei punti razionalmente independenti possa essere ben ordinato.

stessi simboli. Si potrà, sopra la nostra retta, determinare una base minima

$$0,\ \frac{1}{0},\ 1,\ x_1,\ x_2,\ \cdots,\ x_r$$

di punti fra loro razionalmente independenti, tali che ogni altro punto sia un'espressione razionale a coefficienti razionali di essi. La relazione (2), insieme colle condizioni $\phi(0)=0$, $\phi(1)=1$, $\phi(\frac{1}{0})=\frac{1}{0}$, che possono considerarvisi incluse, definirà allora la funzione ϕ per tutti i punti della retta tosto ch'essa sia definita nei punti $x_1, x_2, \cdots, x_r$ per modo che, detti $X_1, X_2, \cdots, X_r$ i punti corrispondenti, — il che si potrà rappresentare colla scrittura

(3) $$X_i = \phi(x_i) \qquad (i=1, 2, \cdots, r)$$

— avvenga che:

1°. Ogni relazione algebrica la quale leghi i punti x_i sia pure soddisfatta se alle x_i si sostituiscano le X_i e reciprocamente ogni relazione algebrica fra le X_i sia soddisfatta pure dalle x_i.

2°. I punti

$$0,\ \frac{1}{0},\ 1,\ X_1,\ X_2,\ \cdots,\ X_r$$

costituiscano a lor volta una base razionale (che sarà necessariamente minima) pei punti della retta, per modo che ciascuno di questi si esprima razionalmente mediante essi.

Nella condizione 1° è evidentemente inclusa quest'altra, che:

3°. Se un medesimo punto si esprime razionalmente in due modi differenti mediante le x_i (o le X_i) le due espressioni che risultano dopo la sostituzione (3) (o la sua inversa) risultino ancora equivalenti.

Invero, l'equivalenza di due espressioni razionali $f_1(1, x_1, x_2, \cdots, x_r)$, $f_2(1, x_1, x_2, \cdots, x_r)$ si traduce in una relazione algebrica, $f_1 - f_2 = 0$, fra le x_i: allora, a causa della condizione 1°, sarà pure

$$f_1(1, X_1, X_2, \cdots, X_r) - f_2(1, X_1, X_2, \cdots, X_r) = 0.$$

VI. Il supporre che fra gli elementi di una base razionale minima passi una relazione algebrica $F(1, x_1, x_2, \cdots, x_r) = 0$, equivale a considerare una geometria di congruenza; equivale cioè a dire che l'espressione $F(1, x_1, x_2, \cdots, x_r)$ rappresenta lo 0 ed appartiene quindi al modulo fondamentale della geometria.* Inversamente una geometria di congruenza il cui modulo fondamentale sia interamente costituito soltanto da polinomi si può considerare come rappresentante di una geometria avente una base razionale, fra i cui elementi sussistano le relazioni algebriche che si ottengono uguagliando a 0 tali polinomi. La cosa è differente quando del modulo fondamentale faccia parte un numero (necessaria-

* È questo il concetto fondamentale della teoria di KRONECKER dei numeri algebrici.

mente intero e primo); e tal differenza appare ben naturale se appena si osserva che, nel primo caso, l'ammissione di un modulo fondamentale equivale ad ammettere che taluno dei punti razionalmente independenti è però scelto per modo che da questi si può ottenere il punto 0 mediante una determinata successione di operazioni razionali (proiezioni e sezioni), mentre nel secondo caso l'ammissione del modulo fondamentale influisce effettivamente sul concetto di retta (e cioè sul concetto delle operazioni razionali fondamentali: proiezioni e sezioni), per modo che per una determinata successione di tali operazioni, effettuate su punti fissati *a priori*, perchè le dette operazioni abbiano senso determinato (i punti $0, \frac{1}{0}, 1$), riconduce da essi al punto 0.* In ogni caso, basta ritornare sul significato e sulla deduzione della (2) per riconoscere che, nel caso delle geometrie di congruenza, in essa l'uguaglianza va ora sostituita con una congruenza rispetto al modulo fondamentale. Si chiami M questo modulo, e si osservi che ciascun punto X_j sarà rappresentato da una classe di espressioni razionali nelle x_i, congrue fra loro rispetto al modulo M; il problema della determinazione di una trasformazione ϕ equivale allora a *determinare una sostituzione*

$$(4) \qquad X_j \equiv \psi_j(x_i) \quad (\text{mod. } M) \qquad (i, j = 1, 2, \cdots, r)$$

tale che

1° *trasformi ogni polinomio del modulo M (in cui alle variabili x_i si pensino sostituite le corrispondenti X_i) in un polinomio del modulo medesimo.*

2° *i punti $0, \frac{1}{0}, 1, X_1, \cdots, X_r$ costituiscano una base razionale dei punti della retta.*

La prima condizione mostra che il modulo fondamentale della geometria, rispetto alla base $0, \frac{1}{0}, 1, X_1, \cdots, X_r$, si otterrà sostituendo semplicemente le lettere X alle x nei polinomi del modulo fondamentale relativo alla base $0, \frac{1}{0}, 1, x_1, \cdots, x_r$; indicando con $\overline{M}$ il risultato di questa sostituzione, la condizione 2° si potrà enunciare chiedendo che *la trasformazione* (4) *abbia una inversa univocamente determinata*

$$(4') \qquad x_i \equiv \Psi_i(X_j) \quad (\text{mod. } \overline{M}).$$

VII. Le x_i e le X_j erano fin qui simboli rappresentanti punti razionalmente independenti della nostra retta. Si interpretino ora per un istante come variabili. Quando del modulo M non faccia parte un numero, la condizione ch'esso sia primo (n°. I) si traduce nel fatto che appartengano ad esso tutti e soli i polinomii che, uguagliati a 0, determinano, nello spazio di coordinate x_i, iper-

---

* I casi già ricordati della $G(2, 2)$ in cui esiste una *terna* armonica di punti e della $G(2, 3)$ in cui esiste la configurazione dei 9 flessi d' una cubica, chiariscono in modo evidente questa osservazione. Come in un piano di soli punti razionali (e quindi reali), i punti delle nostre geometrie si ottengono con sole operazioni razionali (projezioni e sezioni) dai punti di coordinate $0, \frac{1}{0}, 1$: ma punti che per tal generazione risulterebbero necessariamente distinti nell' ordinario piano reale, vengono ora a coincidere.

superficie passanti per una determinata varietà irreduttibile (razionalmente).* Segue allora che *la trasformazione* (4), *in cui si sostituisca il segno* $=$ *al* $\equiv$, *rappresenterà una trasformazione algebrica di questa varietà in sè*, la quale, a causa della esistenza di una inversa univoca (4′) *sarà pure birazionale.* Inversamente ogni trasformazione birazionale a coefficienti razionali della varietà rappresentativa del modulo fondamentale in sè definirà una sostituzione (4) la quale muterà una ipersuperficie per essa varietà in una analoga ipersuperficie, e quindi, operata sopra un polinomio qualunque del modulo, lo muterà in un polinomio del modulo. E questa sostituzione ammetterà una inversa (4′): per ottenerla si considerino le espressioni razionali delle x nelle X che, *sulla varietà rappresentativa del modulo* M, definiscono la trasformazione inversa della (4): saranno esse i secondi membri Ψ della sostituzione (4′): invero il prodotto delle due trasformazioni $X_i = \psi_i(x_j)$, $x_j = \Psi_j(X'_i)$ sarà una trasformazione $X_i = \Theta_i(X'_k)$ la quale, quando le X'_k si interpretano come coordinate di un punto generico della varietà rappresentativa del modulo, deve ridursi all'identità, cosicchè deve essere

$$\Theta_i(X'_k) \equiv X'_k \quad (\text{mod } M')$$

dove M' è il modulo M scritto nelle variabli X' in luogo delle x.† Quindi *ad ogni trasformazione birazionale a coefficienti razionali della nominata varietà in sè corrisponde una trasformazione armonica della nostra geometria.* Varrà quindi il teorema di v. STAUDT quando la varietà rappresentativa del modulo fondamentale non ammetta trasformazioni birazionali a coefficienti razionali in sè.

---

* Invero, non potrebbero tutte queste ipersuperficie avere a comune una varietà riduttibile, altrimenti apparterrebbero al modulo polinomi prodotti di altri non appartenenti ad esso, in quanto rappresentano ipersuperficie passanti per le singole parti soltanto di essa varietà. D'altra parte, per un noto teorema del sig. HILBERT (*Ueber die Theorie der algebraischen Formen*, Mathematische Annalen, vol. 36 (1890), p. 474; KÖNIG, *Einleitung in die allgemeine Theorie der algebraischen Grössen*, p. 366) tutti i primi membri delle equazioni delle ipersuperficie per una varietà determinata costituiscono un modulo. Nè, nel caso nostro, potrebbero le forme del modulo M corrispondere a una parte soltanto delle ipersuperficie per la detta varietà comune, e nemmeno potrebbe tal varietà comune venir a mancare, poichè ancora per un teorema dello HILBERT (*Ueber die vollen Invariantensysteme*, Mathematische Annalen, vol. 42 (1893), p. 320; KÖNIG, l. c, p. 399) ed uno del LASKER (*Zur Theorie der Moduln und Ideale*, Mathematische Annalen, vol. 60 (1905), p. 30; SEVERI, *Su alcune proprietà dei moduli di forme algebriche*, Atti della R. Acc. delle Sc. di Torino, 1906), una conveniente potenza di un polinomio qualunque nel secondo caso, o rappresentante un' ipersuperficie per la varietà considerata nel primo, deve appartenere al modulo: ma il modulo non sarebbe primo (o, più direttamente, non sarebbe soddisfatta la proprietà fondamentale del nostro campo numerico, che un prodotto sia $= 0$ solo se è nullo qualcuno dei fattori) se al modulo potesse appartenere una potenza di un polinomio, e non il polinomio medesimo.

† Invero, posto $\Theta_i(X'_k) = \theta_i(X'_k)/\theta'_i(X'_k)$, il polinomio $\theta_i(X'_k) - X'_i\theta'_i(X'_k)$ dovrà rappresentare una ipersuperficie passante per la varietà considerata e dovrà quindi appartenere al modulo M'; quindi $\theta_i(X'_k) \equiv X'_i\theta'_i(X'_k)$ (mod M') e, poichè certamente $\theta'_i(X'_k)$ non appartiene ad M', $\Theta_i(X'_k) \equiv X'_i$ (mod M').

Una interpretazione delle condizioni 1° e 2° nel caso che il modulo contenga un numero presenta assai maggiori difficoltà.

VIII. Ci volgiamo ora al problema da cui siamo partiti: *Supponendo di considerare una geometria finita, in cui quindi il modulo fondamentale sia della forma*

$$M = [p, F_n(x)]$$

ove p è un numero primo e $F_n(x)$ un polinomio in x a coefficienti interi, di grado n e irreduttibile rispetto al modulo p, qual è il numero massimo di punti $\xi_1, \xi_2, \cdots, \xi_\nu$ tali che il verificarsi della relazione $\phi(\xi_k) = \xi_k$ per ogni $k \leqq i$ non abbia per conseguenza $\phi(\xi_{i+1}) = \xi_{i+1}$, ma il verificarsi dell'uguaglianza*

$$\phi(\xi_k) = \xi_k$$

per tutti questi punti abbia per conseguenza che la trasformazione armonica definita dalla ϕ è l'identità?

In tal modo deve infatti interpretarsi la generalizzazione del teorema di v. Staudt, perchè è ben facile vedere che esistono sulla retta punti tali che ogni trasformazione armonica ϕ che tenga fermi al solito i punti $0, \frac{1}{0}, 1$ e uno di essi è senz'altro l'identità: tale è per esempio il punto x, dove x è la lettera ordinatrice dei polinomi, o, se si vuole, una radice primitiva del campo di Galois; e solo può dubitarsi che possano esistere trasformazioni armoniche ϕ le quali spostino questi punti, tenendo però fermi altri punti della retta, oltre i punti della catena che contiene i punti $0, \frac{1}{0}, 1$. Per risolvere tal questione occorre che ricordiamo anzitutto alcune proprietà dei campi di Galois:

Se ξ_1 è un elemento di un campo di Galois $G(p^n)$ che non sia un numero intero, l'insieme dei polinomi interi in ξ_1, ridotti rispetto al modulo M che definisce il campo, costituisce un campo di Galois $G(p^{n'})$ [che si potrà indicare con $(1, \xi_1)$] contenuto in $G(p^n)$, ed il numero n' è divisore di n. Se poi ξ_2 è un nuovo elemento di $G(p^n)$ non appartenente a $G(p^{n'})$, l'insieme dei polinomi interi in ξ_1, ξ_2, ridotti rispetto al modulo M, costituirà un nuovo campo di Galois $G(p^{n''})$ [che si potrà indicare con $(1, \xi_1, \xi_2)$] contenente $G(p^{n'})$ e contenuto in $G(p^n)$ per modo che n'' sarà divisore di n e n' divisore di n''.†

Si osservi ora che se una trasformazione armonica ϕ trasforma ξ_1 in se

*Sempre quando al modulo appartiene un numero p (necessariamente primo) tutti i coefficienti dei polinomi che costituiscono gli elementi del campo numerico considerato possono supporsi numeri interi per le osservazioni già fatte al No. II.

†Cfr. Dickson, *Linear groups with an exposition of the Galois Field theory*, Leipzig, 1901, pp. 50 e 51. Per riconoscere l'esattezza di queste affermazioni basta osservare che se λ è un elemento non appartenente al campo di Galois $G(p^\nu)$, un campo di Galois contenente λ e $G(p^\nu)$ conterrà almeno i $p^{\nu+1}$ elementi somme degli elementi di $G(p^\nu)$ cogli elementi $h\lambda\,(0 \leqq h < p)$, e se, oltre queste somme, contiene un altro elemento μ, ne conterrà pure $p^{\nu+2}$ ottenuti combinando in simil modo μ con questi $p^{\nu+1}$ e così via.

stesso, trasformerà in sè tutti gli elementi del campo $(1, \xi_1)$, e se trasforma in sè ancora ξ_2, trasformerà pure in sè tutti gli elementi del campo $(1, \xi_1, \xi_2)$ e così via. Ne risulta che *il numero dei punti* ξ_k *definiti nel precedente enunciato è minore o uguale al numero dei termini della massima successione di numeri*

$$n', n'', n''', \cdots, n$$

$(>1$ *e* $\leqq n)$, *ciascuno dei quali sia divisore del seguente;* altrimenti detto, è *minore o uguale al numero dei divisori primi di* n.

Ma si può aggiungere che *questo massimo è sempre raggiunto*, cosicchè al "minore od uguale," si potrà sostituire "*uguale*" senz'altro. Si osservi infatti che, nel caso presente in cui gli elementi della nostra geometria analitica appartengono ad un campo di Galois $G(p^n)$, le condizioni 1° e 2° imposte alla trasformazione (4) equivalgono a dire che

$$(5) \qquad X \equiv x^{p^\nu} \pmod M \qquad (0 \leqq \nu < n).$$

Invero la X, dovendo essere radice della congruenza $F_n(x) \equiv 0 \pmod M$, dovrà avere la forma (5)* e d'altronde l'inversa della (5) sarà data evidentemente da $X^{p^{n-\nu}} \equiv x^{p^n} \equiv x \pmod M$.† Si corrisponderanno per la trasformazione ϕ gli elementi $x^{\mu p^\nu}$ e X^μ; e sarà

$$X^\mu \equiv x^{\mu p^\nu} \equiv x^\mu$$

quando

$$\mu(p^\nu - 1) \equiv 0 \pmod{p^n - 1}.$$

Ora il massimo comun divisore di $p^\nu - 1$ e $p^n - 1$ è della forma $p^l - 1$ ove $\nu = ll'$, $n = l\lambda$ ed l' e λ sono primi fra loro; ed il più piccolo valore di μ per cui questa congruenza è soddisfatta rende $\mu(p^l - 1) = p^n - 1$. Reciprocamente, scelto arbitrariamente l divisore di n e posto $n = l\lambda$, l' primo con λ, $\nu = ll'$, esiste un $\mu = (p^n - 1)/(p^l - 1)$ e quindi $< p^n - 1$ tale che $\mu(p^\nu - 1) \equiv 0 \pmod{p^n - 1}$ e quindi $X^\mu \equiv x^\mu$. Segue che condizione necessaria e sufficiente affinchè la trasformazione (5) lasci fermo qualche punto ad ascissa non numerica è che ν ed n abbiano divisori comuni: se l è il massimo comun divisore di ν ed n resteranno fissi tutti i punti del campo di Galois $(1, x^\mu)$ ove $\mu = (p^n - 1)/(p^l - 1)$: sarà questo un $G(p^l)$.

Fissata quindi arbitrariamente una qualunque successione

$$n', n'', n''', \cdots, n \qquad (n' > 1)$$

di divisori di n *tali che ciascuno di essi sia uguale al precedente moltiplicato per un numero primo, si può ad essa far corrispondere una successione di campi di Galois*

$$G(p^{n'}), G(p^{n''}), G(p^{n'''}) \cdots, G(p^n)$$

---

* SERRET, *Cours d'algèbre supérieure*, 5me édition, 1885, T. 2, p. 180.

† Cf. DICKSON, l. c., p. 11; SERRET, l. c., No. 346, p. 132.

dei quali l'ultimo sia il campo totale dei punti della nostra retta, e ciascuno dei quali contenga tutti i precedenti; e a ciascuno $G(p^{n^{(k)}})$ *di questi campi si possono far corrispondere trasformazioni* $\phi^{(k)}$ *tali che tengano fermi tutti i punti di* $G(p^{n^{(k)}})$ *(e quindi i punti dei campi precedenti) ma spostino ogni punto dei campi successivi, che non appartenga a questi. Una data* ϕ *sarà una* $\phi^{(k)}$ *tosto che essa tenga fermo un punto di* $G(p^{n^{(k)}})$, *non appartenente a* $G(p^{n^{(k-1)}})$, *e sposti un punto di* $G(p^{n^{(k+1)}})$. *Dato* $n^{(k)}$ *il numero delle* $\phi^{(k)}$ *differenti è il numero dei numeri primi con* $n/n^{(k)}$ *e minori di esso.*

Per assicurare che una ϕ *si riduce all'identità occorre verificare al più che essa tien fissi tanti punti, ciascuno razionalmente independente dai precedentemente considerati, quanti sono i divisori primi del numero* n.

Particolarmente notevole è il caso in cui n sia primo; allora, qualunque sia l'elemento ξ di $G(p^n)$, non numero, il campo $(1, \xi)$ è il campo totale $G(p^n)$; quindi se $\phi(\xi) = \xi$, sarà, per ogni altro elemento η, $\phi(\eta) = \eta$. *Se* n *è primo una trasformazione armonica che, oltre ai tre punti* $0, 1/0, 1$ *tenga pur fermo un punto qualunque non appartenente alla catena di questi tre sarà sempre l'identità.*

TORINO, ITALIA, 13 *Ottobre* 1906.
